# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/615,065 | 07/08/2003 | Sung-Ming Yen | 4444-0294PUS1 | 8008 |

2292 7590 03/23/2007
BIRCH,STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

| EXAMINER | |
|---|---|
| SHAN, APRIL YING | |
| ART UNIT | PAPER NUMBER |
| 2135 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | NOTIFICATION DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 03/23/2007 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/23/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

| Office Action Summary | Application No.<br>10/615,065 | Applicant(s)<br>YEN ET AL. | |
|---|---|---|---|
| | Examiner<br>April Y. Shan | Art Unit<br>2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on 28 December 2006.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) 1-3 and 5-10 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-3 and 5-10 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

1. The Applicant's amendment, filed 28 December 2006, has been received, entered into the record, carefully and respectfully considered.

2. As a result of the amendment, claims 1-3 and 5 - 10 have been amended. Claims 4 and 11 have been canceled. Claims 1-3 and 5-10 are now presented for examination.

3. Any objections or rejections not repeated below for record are withdrawn due to Applicant's amendment/explanation/cancellation.

### *Claim Objections*

4. Claims 2-3, 6-7 and 9-10 are objected to because of the following informalities:

a. Claims 2-3, 6-7 and 9-10 are grammatically incomprehensible.

Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-3 and 5-10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

As per **claims 1, 5 and 8**, the Applicant recites "for implementing a modular exponentiation in a cryptographic operation on a digital message in a computer system…". The examiner carefully and respectfully reviews the original disclosure, the Applicant merely discloses in the abstract "provides a method for protecting public key schemes from timing, power and fault attacks" and the original disclosure has no "digital message" at all. Further, the Applicant recites "unconditionally performing a first modular multiplication….unconditionally performing a second modular multiplication…". The examiner finds no support in the original disclosure about "unconditionally" performing the calculations.

As per **claims 2, 6 and 9**, the Applicant recites "…and the first and second examined bits are adjacent binary digits composing said secret exponent key". After carefully reviewing the original disclosure, the Applicant never discloses in the original disclosure a first and second examined bits and they are adjacent binary digits in the original disclosure.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

7. Claims 1-3 and 5-8 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to

which it pertains, or with which it is most nearly connected, to make and/or use the invention.

As per **claims 1, 5 and 8**, as based on the original disclosure, which is not enabling. The steps of executing from the most significant bit of said exponent to the least significant bit of said exponent is critical or essential to the practice of the invention, but not included in the claim(s) and not enabled by the disclosure. See In re Mayhew, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976).

The Applicant recites "unconditionally performing a first modular multiplication and performing a second modular multiplication...outputting..." and it appears to the examiner that amended claims 1, 5 and 8 performing two calculations then output the final result and there is no iteration executing from the most significant bit of said exponent to the least significant bit of said exponent, which is contradicted to the Applicant's original disclosure. For example, in fig. 4 of the original disclosure, the Applicant discloses loop FOR k = w-1 downto 0 DO in step 3. After executing the least significant bit of said exponent, then in step 6 to output S0.

Also, on page 18 of the Applicant's argument, the Applicant states "In other words, the claimed performing steps are always executed in **each iteration of the loop** for computing the modular exponentiation". Therefore, the Applicant's argument again proves to the examiner that executing iteration of the loop is critical and essential step to the current application, but is missing from the amended claims 1, 5 and 8.

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

Claims 1-3 and 5-7 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claim 1**, the preamble recites "implementing a modular exponentiation in a cryptographic operation on a digital message...". However, the body of the claim recites "outputting a final result of the modular exponentiation..." which does not accomplish what the preamble states.

As per **claim 5**, the preamble recites "an apparatus...". However, the body of the claim recites method of steps. Is the Applicant's intention to claim an apparatus or a method?

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

### ***Claim Rejections - 35 USC § 101***

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. Claims 1-3, 5-7 and 8-10 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

**Claims 1-3** are directed to a method for performing a cryptographic operation. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. The claimed steps do not result in a tangible result. Claims 1-3 are rejected as being directed to an abstract idea (i.e., producing non-tangible result) [tangible requirement does require that the claim must recite more than a 101 judicial exception, in that the process must set forth a practical application of that 101 judicial exception to produce a real-world result, Benson, 409 U.S. at 71-72, 175 USPQ at 676-77).

**Claims 5-7** are directed to an apparatus for performing a cryptographic operation. However, it appears that the apparatus would reasonably be interpreted by one of ordinary skill in the art as software, per se. There is no element positively recited as part of the apparatus. Applicant's specification provides no explicit and deliberate definition on any element positively recited as part of the apparatus, and it appears that such would reasonably be interpreted as representative of the software which performs a cryptographic operation on a digital message. As such, it believed that the apparatus of claim 5-7 is reasonably interpreted as functional descriptive material, per se.

**Claims 8-10** are directed to a computer-readable medium for performing a cryptographic operation. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. The claimed logic code does not result in a tangible result. Claims 8-10 are rejected as being directed to an abstract idea (i.e., producing non-tangible result) [tangible requirement does require that the claim must recite more than a 101 judicial exception, in that the process must set forth a practical application of that 101 judicial exception to produce a real-world result, Benson, 409 U.S. at 71-72, 175 USPQ at 676-77).

### *Claim Rejections - 35 USC § 103*

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

14. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a.later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

15. Claims 1-3 and 5-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (U.S. Patent 6,298,442).

As per **claims 1 and 5**, Kocher et al. discloses a method/apparatus for implementing a modular exponentiation in a cryptographic operation on a digital message in a computer system, the modular exponentiation involving a secret exponent key, comprising:

unconditionally performing a first modular multiplication by multiplying a first multiplicand variable by a first multiplier variable followed by a modular operation and storing result of the first modular multiplication into a first variable (step 125 in fig. 1 and "where the device updates R by computing R=RQ mod n" – e.g. col. 5, ll. 66-67);

conditionally performing a second modular multiplication by multiplying a second multiplicand variable by a second multiplier variable followed by the modular operation and storing result of the second modular multiplication into the first variable (e.g. fig. 1 and col. 6, ll. 20 – 53); and outputting a final result of the modular exponentiation from a memory location of the first variable in the computer system (step 160 in fig. 1 and "...where the final value R is returned" – e.g. col. 6, l. 43)

wherein the first variable, the first multiplicand variable and the second multiplicand variable are purposely arranged to be the identical variable (Please note in step 125 in fig. 1, R = RQ mod n and R is the first multiplicand variable and the second multiplicand variable. They are the identical variable).

Kocher et al. does not expressly disclose unconditionally performing a second modular multiplication.

However, in another embodiments of the Kocher reference in col. 7, ll. 26-50 and col. 8, ll. 55-65, Kocher discloses unconditionally performing a second modular multiplication.

It would have been obvious to a person with ordinary skill in the art to incorporate Kocher's other embodiments of unconditionally performing a second modular multiplication into Kocher's method/apparatus.

The motivation of doing so would have been "reduce memory requirements of the modular exponentiator with little or no performance penalty by re-encoding equivalent representation", as disclosed by Kocher (col. 8, ll. 55-58) and "such operation-based encoding may also be used to make variants of the method of FIG. 1 that are slightly simpler (and hence more compact)", as disclosed by Kocher (col. 7, ll. 51-52)

As per **claims 2 and 6**, Kocher further discloses wherein the first multiplier variable is respectively set to 1 and said digital message if a first examined bit is respectively equal to 1 and 0; the second multiplier variable is respectively set to 1 and said digital message if a second examined bit is respectively equal to 0 and 1; and the first and second examined bits are adjacent binary digits composing said secret exponent key (e.g. col. 5, l. 35 – col. 6, l. 63 and fig. 1)

As per **claims 3 and 7**, Kocher further discloses characterized by that no multiplier of any multiplication operation is arranged to store an intermediate result of any modular multiplication operation such that the method is resistant to M safe error attacks (e.g. fig. 1)

As per **claims 8-10**, Kocher discloses the claimed method of steps as applied above in claims 1-3. Therefore, Kocher discloses the claimed computer program embodied in a computer –readable medium for carrying out the method of steps.

### ***Response to Arguments***

16. Applicant's arguments filed 28 December 2006 have been fully considered but they are not persuasive.

- Applicant argues on pages 16-17, "..The Examiner's attention is drawn to the "safe harbor" section of MPEP 2106(IV)(B2)...Claims 1-3..outputs...Claims 5-7..."

First, the examiner respectfully points out the office is currently using MPEP 5th version and what the Applicant cited is not found under MPEP 5th version 2106(IV)(B2).

Second, the examiner respectfully points out the body of the amended claims 1 and 8 recite "outputting a final result of the modular exponentiation..." which does **not** accomplish what the Applicant states in the argument "the method outputs an **encrypted digital message**...". Therefore, final result in claims 1-3 and 8-10 are still abstract as it would just be mathematics caculations. Therefore, claims 1-3 and 8-10 are non-statutory.

Third, the examiner respectfully points out the amended claims 5-7 are not clear whether they are apparatus claims or method claims. If treated as apparatus claims, besides abstract ideas, claims 5-7 are also software pro se. Therefore, claims 5-7 are non-statutory.

- Applicant argues "Kocher and Benoit...fails to teach using the same variable for the modular-multiplying result and the multiplying multiplicand...unconditionally to achieve a branchless computer program..." on pages 18-19.

  The examiner respectfully addressed the above argument in the above 112 and 103 rejections.

### *Conclusion*

17. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a)..

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

### *Contact Information*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

16 March, 2007
AYS

HOSUK SONG
PRIMARY EXAMINER